IN THE CLAIMS

Claim 1 (currently amended) A method of providing a digital file~~data~~ from a source system to an embedded system in a secure manner, comprising the steps of:

combining the digital file~~data~~ with header information including a target identifier corresponding to the embedded system;

providing the combined digital file~~data~~ with header information to the embedded system; and

verifying the target identifier before the embedded system is enabled to ~~load the digital data~~install said digital file on the embedded system.

Claim 2 (original) The method as defined in claim 1 wherein the target identifier is a text name corresponding to an end user of an Internet based service.

Claim 3 (currently amended) The method as defined in claim 1 wherein said target identifier includes a revision level respecting said digital file~~data~~.

Claim 4 (currently amended) A method of providing a digital file~~data~~ from a source system to an embedded system in a secure manner, comprising the steps of:

combining the ~~data~~digital file with header information including a target identifier corresponding to the embedded system;

signing the combined digital file~~data~~ with header information with a digital signature corresponding to the source system, the digital signature being added to the header information;

providing the combined digital file~~data~~ with header information to the embedded system; and

verifying the digital signature and the target identifier before the embedded system is enabled to ~~load the digital data~~install the digital file on the embedded system.

Claim 5 (currently amended) The method as defined in claim 4, wherein the step of signing the combined digital file~~data~~ with header information uses a private cryptographic key associated with the source system to generate the digital signature.

PAGE 5/13 * RCVD AT 1/24/2006 10:03:02 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/29 * DNIS:2738300 * CSID:613 230 8821 * DURATION (mm-ss):02-46

Claim 6 (original) The method as defined in claim 5 wherein the step of verifying the digital signature uses a public key corresponding to the private cryptographic key.

Claim 7 (currently amended) An embedded system that uses a target state header to validate uploaded files, the system comprising:

means to combine the files to be uploaded with the target state header;

means to provide the files with the target state header to the embedded system; and

verifying means to verify the target state header before the files are ~~uploaded to~~installed on the embedded system.

Claim 8 (currently amended) The embedded system as defined in claim 7 having means to provide a digital signature for use in verifying the files before ~~uploading to~~installing the files on the embedded system.

Claim 9 (original) The embedded system as defined in claim 8 having public keying infrastructure for distributing public keying information to said embedded system.

Claim 10 (original) The embedded system as defined in claim 9 having software for performing signature generation and verification.

Claim 11 (original) The embedded system as defined in claim 7 for use in conducting transactions on the Internet.

Claim 12 (original) The embedded system as defined in claim 11 wherein said transactions include the purchase and download of software.

Claim 13 (original) The embedded system as defined in claim 11 wherein said transactions include online banking.

Claim 14 (original) The embedded system as defined in claim 11 wherein said transactions include the installation of software revisions in network nodes.

PAGE 6/13 * RCVD AT 1/24/2006 10:03:02 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/29 * DNIS:2738300 * CSID:613 230 8821 * DURATION (mm-ss):02-46

Claim 15 (currently amended) The embedded system as defined in claim ~~11~~14 wherein said network nodes include wireless telephones.

PAGE 7/13 * RCVD AT 1/24/2006 10:03:02 AM [Eastern Standard Time] * SVR:USPTO-EFXRF-6/29 * DNIS:2738300 * CSID:613 230 8821 * DURATION (mm-ss):02-46